REMARKS

Applicants appreciate the detailed examination evidenced by the Office Action mailed February 17, 2005 (hereinafter "Office Action"). In response, Applicants have amended the Abstract to address the Examiner's objections. Also, independent Claims 1, 26, 27, 28, 31 and 32 have been amended to clarify that the common nonce is obtained "from an entity other than the client or the plurality of servers." Accordingly, Applicants respectfully request reconsideration and withdrawal of the rejections of Claims 1-32 for at least the reasons provided below.

The Specification Objections

The Abstract of the Disclosure has been objected to for repeating information which can be implied. *See* Office Action, Pages 2-3. In response, Applicants have amended the Abstract of the Disclosure to remove such information and to correct minor errors therein. Accordingly, Applicants respectfully request withdrawal of the objections.

The Claim Objections

Claims 5-22 have been objected to for failing to comply with the numbering standard set forth in 37 C.F.R. 1.75(c). *See* Office Action, Page 3. Applicants sincerely appreciate the Examiner's participation in the telephonic interview of May 5, 2005, in which the objections to Claims 5-22 were discussed. In particular, Applicants appreciate the Examiner's explanation of the numbering standard, and the indication that no further action is required to address the claim objections. Accordingly, Applicants respectfully request withdrawal of the objections.

Independent Claims 28, 31 and 32 Are Patentable Over Ford

Independent Claims 28, 31 and 32 stand rejected under 35 U.S.C. §102(e) as anticipated by U.S. Patent No. 6,829,356 to Ford (hereinafter "Ford"). Claim 28 as amended recites:

> A method of authenticating a client, comprising:

> receiving at a server of a plurality of servers, a common nonce which is associated with each of the plurality of servers from an entity other than the client or the plurality of servers, the common nonce being signed by the client; and
>
> authenticating the client based on the received signed common nonce.

(*Emphasis added*).

Applicants submit that Ford does not disclose all of the recitations of Claim 28 as amended. Ford appears to be directed to secure regeneration of a user's "strong" secret data (such as the user's private cryptographic key) when the user supplies "weak" secret data (such as a user-chosen password), for example, in instances where the user accesses a particular computer network or servers from many different locations or clients. *See* Ford, Col. 1, lines 20-34. As such, the different client terminals can securely obtain a copy of the user's private data for authentication with the network and/or servers. To verify that the strong secret data K was correctly recovered, the client **220** supplies proof data to the servers **130A**...**130N** based on nonces n(i) received from the servers **130A**...**130N**. *See* Ford, Fig. 6. In particular, the cited portion of Ford recites:

> [T]he recovery client **220** can generate **650** proof data by digitally signing a message containing the various nonces n(i) using the user's recovered private key $Priv_u$. Each verification server verifies **660** successful recovery of the strong secret data K by verifying the digital signature using the user's public key Pub_u, and then verifying that the correct nonce n(i) is included in the message.

See Ford, Col. 15, lines 56-65. The Office Action appears to assert that the "message containing the various nonces" described in Ford may be considered a "common nonce" as recited by Claim 28.

However, Ford does not appear to disclose a common nonce that is received "from an entity other than the client or the plurality of servers", as recited by Claim 28 as amended. Rather, as stated in the cited portions of Ford, it is the recovery client **220** that generates and transmits the digitally signed message containing the various nonces. In other words, if the message containing the various nonces is considered to be a common nonce, as asserted by the Office Action, the common nonce of Ford is received from the client **220**. Moreover, Ford appears to describe authentication directly between the client **220** and the servers

130A...130N, and as such, does not appear to contemplate receiving a common nonce and/or other messages related to authentication from any other entities.

Accordingly, Applicants submit that Ford does not disclose or suggest all of the recitations of Claim 28 as amended. For at least this reason, Claim 28 is patentable over Ford. Applicants further submit that Claims 31 and 32 as amended contain system and computer program recitations corresponding to the method of Claim 28. As such, Claims 31 and 32 are also patentable over Ford for at least similar reasons.

Independent Claims 1, 26 and 27 Are Patentable Over Ford and Blakely

Independent Claims 1, 26 and 27 stand rejected under 35 U.S.C. §103(a) as obvious over Ford in view of U.S. Patent No. 6,067,623 to Blakely, III et al. (hereinafter "Blakely"). Claim 1 as amended recites:

> A method for a middle-tier server to impersonate a client to a plurality of servers, the method comprising:
> obtaining a common nonce associated with each of the plurality of servers from an entity other than the client or the plurality of servers;
> providing the common nonce to the client;
> receiving the common nonce signed by the client at the middle-tier server; and
> providing the signed common nonce as a signature for transactions from the client to the plurality of servers so as to authenticate the client to the plurality of servers.

Applicants submit that neither Ford nor Blakely discloses or suggests all of the recitations of Claim 1 as amended. As discussed above, Ford does not appear to disclose or suggest obtaining a common nonce "from an entity other than the client or the plurality of servers", as recited by Claim 1. Moreover, the Office Action concedes that Ford does not disclose or suggest "providing the common nonce to the client" or " receiving the common nonce signed by the client at the middle-tier server". *See* Office Action, Page 5.

Nor does Blakely appear to supply the missing recitations. Blakely describes a middle tier server which appears to authenticate a user with an enterprise resource based on client authorization with the middle tier server. *See* Blakely, Col. 3, lines 4-8. As described in Blakely, "[t]he middle tier server according to the present invention accesses resources on behalf of a client by mapping the credentials used to access the [middle tier] server into

credentials for accessing the resource." *See* Blakely, Col. 4. lines 18-21. More specifically, Blakely states:

> [T]he middle tier server authenticates the user using its preferred authentication mechanism **126** then it passes the user identity to the credential transformer **124**...and causes credential transformer **124** to attempt to map the authenticated user id to an id for the enterprise resource using id map file **134**...Access to an enterprise resource requires authentication with that resource.

See Blakely, Col. 4, line 60 to Col. 5, line 18. In other words, Blakely appears to describe two authentication operations performed sequentially: a first authentication operation between the client and the middle tier server, and then a second authentication operation between the middle tier server and the enterprise resource. The second authentication operation is based on mapping the authenticated user identification to an identification for the particular enterprise resource.

Accordingly, nowhere does Blakely appear to describe the use of "a common nonce associated with each of the plurality of servers" in the above-described authentication operations. Blakely also does not appear to disclose or suggest "providing the common nonce to the client", and "receiving the common nonce signed by the client at the middle-tier server" as recited by Claim 1 as amended.

Moreover, Claim 1 further recites "providing the signed common nonce...from the client to the plurality of servers so as to authenticate the client to the plurality of servers. Thus, according to Claim 1, authentication of the client may be performed at multiple servers in parallel based on one signed common nonce, rather than sequentially between the client and the middle tier server and then between the middle tier server and each of the resources, as described by Blakely. As such, Applicants submit that Blakely also teaches away from the recitations of Claim 1.

Applicants further submit that one would not be motivated to combine the teachings of Blakely with those of Ford, and moreover, that such a combination would not operate in the manner intended. As described above, Ford relates to direct client-server authentication, while Blakely relates to a middle tier server that maps credentials received from a client into credentials for authentication with back end servers/resources. The Office Action asserts that

it would be obvious to combine the middle-tier server of Blakely with the authentication system of Ford "to reduce network traffic between the client and servers." *See* Office Action, Page 5.

However, the Office Action provides no evidence from the prior art as to how the middle tier server of Blakely would be applied to the system of Ford. As the client **220** of Ford requires the nonces n(i) from the servers **130A...130N** to generate the proof data, and as the servers **130A...130N** require the proof data from the client **220** for verification, the inclusion of a middle tier server would not appear to reduce traffic between the client **220** and the servers **130A...130N**. Furthermore, if the middle tier server of Blakely were combined with the system of Ford, the middle tier server would receive the message containing the nonces from the client **220** of Ford, and would map the message to individual messages for each of the servers **130A...130N**, thereby obscuring verification of the respective nonces at the servers **130A...130N**. Accordingly, Applicants submit that it would not be obvious to combine the teachings of Blakely with those of Ford, and moreover, that the references teach away from such a combination.

Thus, as the combination of Ford and Blakely does not disclose or suggest all of the recitations of Claim 1 as amended, and as there is no motivation to combine the two, Applicants submit that Claim 1 is patentable over the combination of Ford and Blakely. Applicants further submit that Claims 26 and 27 as amended contain system and computer program recitations corresponding to the method of Claim 1. As such, Claims 26 and 27 are also patentable for at least similar reasons.

Many of the Dependent Claims Are Separately Patentable

Applicants submit that dependent Claims 2-25 and 29-30 are patentable at least by virtue of the patentability of independent Claims 1 and 28 from which they respectively depend. Applicants further submit that several other of the dependent claims are also separately patentable.

For example, Claim 23 stands rejected under 35 U.S.C. §103(a) as obvious over the combination of Ford and Blakely in further view of U.S. Patent 6,052,784 to Day (hereinafter

"Day"). Claim 23 recites, in part, "obtaining the common nonce from a party trusted by the middle-tier server and the plurality of servers, the common nonce being signed by the trusted party."

The Office Action concedes that the combination of Ford and Blakely fails to describe receiving a common nonce from such a trusted party, and relies on Day to provide the missing recitation. *See* Office Action, Page 12. In the portions cited by the Office Action, Day discloses a trusted third party certification authority that establishes the authenticity of a certificate from a first resource. *See* Day, Col. 3, lines 44-46. More specifically, as described in Day, "[a] first certificate is created when the first resource selects a first nonce and submits it to the certification authority...The certification authority signs the first nonce...to produce an authenticated first certificate that is returned to the first resource." *See* Day, Col. 3, lines 46-54. As such, Day appears to describe that the first resource obtains a first nonce signed by a trusted party. However, nowhere does Day appear to disclose or suggest "obtaining the common nonce from a party trusted by the middle-tier server and the plurality of servers", as recited by Claim 23 (*Emphasis added*).

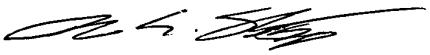
The Office Action asserts that it would be obvious to combine the certification authority of Day with the teachings of Ford and Blakely to have "the nonce challenges signed by a certification authority prior to sending the challenge to the client". *See* Office Action, Page 12. However, the Office Action provides no evidence from the prior art as to how the certification authority of Day would be applied to the middle tier server of Blakely and the system of Ford. Moreover, even if the teachings of Ford, Blakely, and Day were combined, the combination would not disclose all of the recitations of Claim 23. More specifically, as discussed above with reference to Claim 28, Ford describes generating a message containing various nonces, which the Office Action asserts is common nonce, at the client **220**. As such, even if the certification authority of Day was combined with the teachings of Ford and Blakely, the common nonce would be obtained by the certification authority from the client 220, not from "a party trusted by the middle-tier server and the plurality of servers", as recited by Claim 23.

Accordingly, Applicants submit that the combination of Ford, Blakely, and Day does not disclose or suggest all of the recitations of Claim 23. As such, Applicants submit that Claim 23 is patentable over the cited references for at least these reasons. In addition, Claim 29 similarly recites "[t]he method of Claim 28, wherein the common nonce is provided by a trusted third party." As such, Applicants further submit that Claim 29 is thus patentable over the cited references for at least similar reasons.

Conclusion

Accordingly, Applicants submit that the rejections of the claims are overcome for at least the reasons discussed above, and that the claims are, therefore, in condition for allowance, which is respectfully requested. Applicants encourage the Examiner to contact the undersigned by telephone to resolve any remaining issues.

Respectfully submitted,

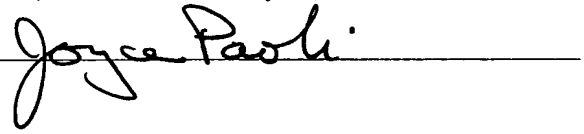


Rohan G. Sabapathypillai
Registration No. 51,074

USPTO Customer No. 20792
Myers Bigel Sibley & Sajovec, P.A.
Post Office Box 37428
Raleigh, NC 27627
Telephone (919) 854-1400
Facsimile (919) 854-1401

CERTIFICATE OF MAILING UNDER 37 C.F.R. § 1.8

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: MAIL STOP AMENDMENT, Commissioner for Patents, P.O. Box 1450, Alexandria, VA, 22313-1450, on May 17, 2005 .



Joyce Paoli